

In our digital world, it may be impossible to protect personal information.

Is Anything Private Anymore?

By Sean Flynn

Published: September 16, 2007

Kevin Bankston was a closet smoker who hid his habit by sneaking cigarettes outside his San Francisco office. He expected anonymity on a big city street. But in 2005, an online mapping service that provided ground-level photographs captured him smoking—and made the image available to anyone on the Internet. This year, Google's Street View project caught him again.

Coincidence? Absolutely. Yet Bankston's twice-documented smoking highlights a wider phenomenon: Privacy is a withering commodity for all of us.

What you buy, where you go, whom you call, the Web sites you visit, the e-mails you send—all of that information can be monitored and logged. "When you're out in public, it's becoming a near certainty that your image will be captured," says (the newly nonsmoking) Bankston.

Should you care? I've interviewed numerous people on all sides of the privacy debate to find out just how wary we should be.

One thing is clear: In today's world, maintaining a cocoon of privacy simply isn't practical. Need a mortgage or a car loan? A legitimate lender is going to verify a wealth of private information, including your name and address, date of birth, Social Security number and credit history. We all make daily trade-offs for convenience and thrift: Electronic tollbooths mean you don't have to wait in the cash-only lane, but your travel habits will be tracked. The Piggly Wiggly discount card saves you \$206 on your annual grocery bill, but it counts how many doughnuts and six-packs you buy. MySpace posts make it easy to keep in touch with friends, but your comments live on.

So how do you live in a digital world and still maintain a semblance of privacy? Experts say it's crucial to recognize that those bits of data are permanent—a trail of electronic crumbs that is never swept away, available to anyone with the skills and inclination to sniff it out.

Privacy may not feel like much of an issue for those in their teens and 20s. They've grown up chronicling their lives on popular social networking sites like MySpace or Facebook for easy retrieval by friends and strangers alike. But some young people don't realize that what was funny to college buddies might not amuse a law-firm recruiter. Employers regularly research job applicants on the Internet. Some colleges are helping students prepare: Duke University hosts seminars on how to clean up a Facebook account. "You learn why posting pictures of you riding the mechanical bull at Shooters is a bad idea," says Sarah Ball, a senior whose own page is secure and clean.

Amy Pumbo, 22, restricted her page on Facebook to 100 or so people who knew her password. "It was a way for me to keep in touch with friends all over the country," she says. But after she was crowned Miss New Jersey in June, someone downloaded pictures of her and threatened blackmail. She thwarted the attempt by releasing the photos herself (they're quite innocent) but suffered weeks of embarrassment.

"I know how easy it is for someone to take advantage of you on the Internet," says Pumbo. "The Web is a place where people can destroy your reputation if you're not careful."

In fact, all kinds of transgressions now are easily retrievable. An employee at a New York City bank watched his reputation shrink when his colleagues pulled up an article from a small-town newspaper about his drunk-driving arrest two years earlier. Divorce lawyers have been issuing subpoenas for electronic tollbooth records to use in custody cases. (You say you're home at 6 p.m. to have dinner with the kids, but Fast Lane says you're getting off the Massachusetts Turnpike at 7 p.m.) Abbe L. Ross, a divorce lawyer in Boston, finds a gold mine in computers: financial data, e-mails, what Web sites a soon-to-be-ex spouse looks at and for how long. "I love to look through hard drives," she says.

Details about you already are stashed in enormous databases. Unless you pay cash for everything, data brokers almost certainly have compiled a profile of you that will be bought and sold dozens of times to marketers and direct-mail firms. "There's almost nothing

they can't find out about you," says Jack Dunning, who worked in the junk-mail business for 35 years. Right now, there are roughly 50,000 such lists for sale in a \$4 billion a year industry. Now junk mail is going digital: Companies can use personal profiles and records from Internet search engines to tailor advertising—both what you see and precisely when you see it—to individual consumers.

And new databases are being created all the time. Most of the major proposals for health-care reform, for example, include compiling medical records into easily and widely accessible digital files. In July, the FBI requested \$5 million to pay the major phone companies to maintain logs of your calls—information the Feds can't legally stockpile themselves but might find useful later.

Surveillance cameras are increasingly ubiquitous in our post-9/11 world. Indeed, New York City plans to ring the financial district with them, as central London did several years ago.

Of course, there are upsides. London's network of cameras helped capture failed car bombers in June. And streamlined electronic medical records would make health care safer and more efficient.

Still, most experts say we need to be vigilant about the increasing encroachments on our privacy.

The ability to collect information and images has outpaced the security available to protect them. Since January 2005, nearly 160 million personal records have been stolen or inadvertently posted online.

And even if information stays secure, the big question remains: Who should be allowed to access these databases? The FBI might find evidence against a few bad guys in millions of phone records, but the government could track all of your calls too. (President Bush has acknowledged that the National Security Agency tapped phone calls, though whose and how many is unknown.)

Even more disturbing: All of those data files can be linked and cross-referenced. At the 2001 Super Bowl in Tampa, fans were scanned with cameras linked to facial-recognition software in a hunt for suspected terrorists. Some privacy advocates worry that police could videotape anti-war marches and create a library of digital faces or start mining Web pages for personal information.

Kevin Bankston was only caught smoking, but he's worried about larger implications: "The issue isn't whether you have anything to hide," he says. "The issue is whether the lack of privacy would give the government an inordinate amount of power over the populace. This is about maintaining the privacy necessary for us to flourish as a free society."

How To Protect Your Privacy

No one is going to protect your privacy for you. Here are some ways to take control:

Be stingy with personal information. Don't readily give a cashier your address, phone number or Social Security number. Always ask how the information will be used.

Be vigilant in cyberspace. A basic firewall is a must for your home computer. Never give any personal information in response to an e-mail.

Practice anonymity. Want the benefits of the grocery store's discount card without leaving a record of every Twinkie you buy? Ask to sign up as A. Nonymous.

Learn more. Do you have specific questions about privacy or feel that yours has been violated? Visit privacyrights.org for more information.

Are privacy issues a major concern to you? Give specific examples of what things/actions you feel violate your privacy.